EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN RE: APPLICATION FOR AN ORDER PURSUANT TO 28 U.S.C. § 1782 TO CONDUCT DISCOVERY IN AID OF A FOREIGN PROCEEDING	Case No.:

DECLARATION OF MICHAEL JASON LEE IN SUPPORT OF APPLICATION FOR AN ORDER PURSUANT TO 28 U.S.C. § 1782 TO CONDUCT DISCOVERY FOR A FOREIGN PROCEEDING

I, Michael Jason Lee, declare:

1. I am an attorney duly licensed to practice law before all State and Federal courts in the State of California and am admitted to practice before this Court. I am counsel for Applicant with respect to his Application to Conduct Discovery Pursuant to 28 U.S.C. § 1782 (the "Application").

2. I have personal knowledge of all facts alleged herein, except as to matters stated on information and belief, and as to those matters, I believe them to be true. If called to testify with regard to the facts alleged herein, I could do so competently.

3. On behalf of Applicant, I worked with the law firm of Rajah & Tann Singapore LLP to obtain a sealed injunction and disclosure order from the General Division of the High Court of the Republic of Singapore.

4. On June 10 and 16, 2021, Binance produced data in response to the Order issued by the Singaporean court. Since that time, the Singapore court has issued numerous discovery and freeze orders, with the most recent Order issued to an exchange in receipt of Applicant's stolen assets in June 2022.

5. On June 11, 2021, Binance produced extensive documentation responsive to the High Court's order. The data received from Binance establishes that on March 29, 2021—just five days after the first movement of the stolen BTC—an individual created an account with Binance, later providing what appears to be the fraudulent identity information of a Russian

woman (Ms. Kholopova). The account was accessed numerous times using VPNs.

6. The pattern of deposits, transactions, and withdrawals associated with the Binance account evidence an intent to launder Applicant's stolen funds.

7. The records produced by Binance also showed that the individual or individuals in control of Applicant's stolen assets used a customer-specific deposit address with Binance beginning with bc1q3- ("bc1q3").

8. Analysis of the publicly available blockchain records associated with bc1q3 revealed that prior to the deposit of Applicant's stolen funds, the Binance account had received deposits from a different source.

9. Analysis of the relevant blockchain records showed that whoever sent BTC to the Binance account receiving Applicant's stolen funds had also made three deposits to ChangeHero, a Hong Kong-based business that allows users to immediately exchange a given digital asset (e.g., bitcoin) to another digital asset (e.g., Litecoin) without any user verification (e.g., collection of the user's legal name, address, etc.).

10. ChangeHero provided Applicant's third-party investigative service with data regarding the deposits, identifying 167.99.184.140 as the IP Address used to connect to the exchange service.

11. Applicant seeks the assistance of this Court in obtaining information critical to the recovery of his funds. A copy of Applicant's proposed requests and subpoena to DigitalOcean are attached to the Application as "Exhibit C."

12. Discovery produced by Binance pursuant to an order of the General Division of the High Court of the Republic of Singapore, along with analysis of publicly available blockchain records, identify Respondent as providing VPN services to an individual or individuals believed be involved with the theft of Applicant's assets.

13. Applicant believes DigitalOcean possesses information that would reveal the actual identity of those involved in the theft of Applicant's assets.

14. Among other things, DigitalOcean's website indicates that it may possess: "the

email address currently assigned to the account[;] first name, last name and phone number[;] the PayPal or Stripe transaction information for purchases[; and] physical address." Likewise, because DigitalOcean is a for-profit business offering subscription services, DigitalOcean may possess payment and personal identifying information connected to the individual or individuals responsible for the theft.

15. Such information will likely be unavailable from any other source—according to Respondent's own website, running a "private VPN server [through DigitalOcean] . . . prevent[s] third parties from being able to log your traffic" and is touted as offering "total privacy."

16. DigitalOcean is a publicly traded Delaware corporation headquartered at 101 6th Avenue, New York, NY 10013.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 15 day of July 2022, in San Diego, California.

/s/ Michael Jason Lee, Esq.